

Not for publication until released by the subcommittee

Prepared Statement of

Ken Scheflen

Director, Defense Manpower Data Center (East)

**Before the Government Reform Subcommittee on Technology,
Information Policy, Intergovernmental Relations and the Census**

**Oversight Hearing on “Advancements in Smart Card and Biometric
Technology”**

September 9, 2003



Biography

1600 Wilson Blvd., Suite 400
Arlington, VA 22209-2593



KENNETH C. SCHEFLEN
Director
Defense Manpower Data Center

A member of the Senior Executive Service, Mr. Scheflen is the Director of the Defense Manpower Data Center (DMDC), a position he has held since 1977. As such, he is deeply involved in both the management and technical aspects of programs which he supervises. DMDC, which was established 1974, collects and maintains automated data about DoD-affiliated personnel, manpower requirements, and the financial transactions of the Department. DMDC, now a part of the Defense Human Resource Activity (DHRA), uses this automated data to support a variety of DoD-wide programs: the DEERS and RAPIDS programs; development of the ASVAB and other tests for entrance into the military; (DORS); actuarial analysis of the costs of the DoD military retirement system; the identification of individuals owing debts to the Federal government who are receiving Federal compensation; and the detection and prevention of fraud and erroneous payments in the DoD financial system. In addition, DMDC operates a large personnel survey program, tracks military personnel in joint-duty assignments, and develops and manages systems to track the evacuation and repatriation of non-combatant personnel. Since FY98, DMDC has also been the host for the Common Access Card Office, formerly the DoD Smart Card Technology Office, which is in the process of converting the current military ID card to a smart card containing PKI certificates needed to secure the DoD information technology infrastructure and other applications. This project is widely regarded as the most advanced large-scale smart card program in the world.

Mr. Scheflen received undergraduate and graduate degrees from Yale University in Psychology (1968) and Administrative Sciences (1969), respectively. Prior to joining the Defense Department in 1974, he was employed on the corporate personnel staffs of Ford Motor Company in Dearborn, Michigan and the Boise Cascade Corporation in Boise, Idaho. He came to Washington in 1971 to work for the Human Resources Research Organization (HUMRRO), rising to the rank of Senior Scientist and Program Director prior to joining DoD.

Mr. Scheflen was presented the Secretary of Defense Meritorious Civilian Service Award in 1987 and again in 2001, and in 1996 and again in 2001 was conferred the Presidential Rank of Meritorious Executive. He is a member of the American Society of Access Professionals and is a recognized expert on Freedom of Information and Privacy issues, especially with respect to

automated records. As a noted expert on military manpower and personnel issues, he frequently represents DoD in a number of international forums.

Good morning. As the Director of the Defense Manpower Data Center (DMDC), I am responsible for the development, fielding, and maintenance of a number of DoD-wide systems. I will discuss two of these systems today: The Common Access Card commonly referred to as the CAC, and the Biometric Identification Systems or BIDS.

The CAC is a multi-technology chip-based card or “smart card” which is rapidly replacing the existing military identification/ Geneva Convention card for all uniformed service personnel. It is also being given to DoD civilian employees, Selected Reserve and to contractors who require physical access to DoD facilities or otherwise require logical access to DoD systems. This is the first time there has been a standard ID card for either of these populations. DMDC also continues to field the systems which give ID cards to military retirees and family members of active, reserve, and retired personnel. In all, the DoD issues about 4 million ID cards each year and we have over 11 million people with DoD identification cards. The CAC will be issued to about one-third of the overall population or approximately 4 million people.

I would like to take a moment to summarize the status of the CAC roll out and to discuss a few of the technical issues involved. The CAC is the most advanced major smart card program in the world and has been the recipient of twelve major US and international awards including the highly coveted Federal Leadership or “Gracie” award and for being a Computerworld Honors Worldwide Finalist. It is also one of the few major programs doing local rather than centralized card production and issuance. This is due to the importance of the card to military-affiliated people and to the far flung nature of the DoD enterprise. In order to prepare the infrastructure to issue CACs, installers visited 945 locations in twenty-seven countries to install hardware and

software and train operators on how to use the new system. This infrastructure roll out was completed in July 2003 after about an 18 month effort. CAC cards are issued as soon as the equipment has been installed and to date over 3 million have been issued at a rate of 10-15,000 per day and rising.

At DMDC we like to say that we are in the “identity management” business as opposed to the ID card business. It is very clear that the events of 911 and the subsequent investigations have shown how easily obtainable both genuine and forged documents purporting to assert identity are to acquire. Indeed, there is no easy solution to the world-wide problem of knowing exactly who each person is with absolute certainty and binding that person to an identity document or documents with absolute certainty. DoD has a better chance of doing this than most other organizations because of the vetting that its members go through during the enlistment or hiring process. However, even our process is not perfect and we continue to make improvements to our business processes to take advantage of cutting edge technologies. The CAC, one such new technology, is designed to securely bind the identity of a person encountered in a “face-to-face” situation with a highly secure identity card. The CAC contains two bar codes, a magnetic stripe, printed material, digital photograph and an integrated circuit chip (ICC). It is this latter feature which makes it a Smart Card and which makes it possible to use cryptographic tools to log on to a computer, assert one’s identity, conduct secure e-business and e-gov and digitally sign and encrypt email. If used properly in a multi-factor system it can also be used as a physical access tool. In order to actually use the CAC for these purposes, it is necessary for DoD to roll out additional infrastructure-card readers and desk-top middleware and software to enable authentication to web sites using the CAC’s digital certificates. This roll out, which is the

responsibility of the individual services and components, is also well under way with over a million workstations now having the required hardware and software.

I mentioned earlier that we are in the identity management business and that we need to have high assurance that the in-the-flesh person we securely bind to CAC credentials is who he or she purports to be. Identity verification is key and this is one reason why we insist on a face-to-face interaction in addition the presentation of an existing ID card or other credential. Going even further, we have been capturing digital fingerprints on military personnel for approximately four years and thus have prints on most all uniformed members. As part of the CAC issuance we capture prints on civilian and contractor personnel. At re-issuance, which is at intervals no greater than three years, the system does a fingerprint check between the live person and the data base to ensure it is the same person. In the event of a non-match, which can occur for a number of reasons, the operator is required to take additional steps to verify identity before issuing a card. DMDC is working to receive digital fingerprints captured at our enlistment processing stations and transmit them to the FBI for criminal records checks prior to entry. These prints would be used to verify identity the first time a person was issued a CAC, further strengthening the identity management process. DMDC is also experimenting with facial recognition software to permit comparisons of digital images in the data base with camera images of the live person for use in cases where fingerprints do not match or are not used, as is the case for family member cards. While considerable investigation or the utility of other biometric measures is going on in the DoD under the auspices of the DoD Biometrics Management Office, current plans for the CAC are limited to fingerprints and facial recognition.

DMDC is engaged in other projects which make use of both identity cards, CAC as well as others, and biometrics. The best developed of these is the system known as BIDS or the Biometric Identification System. This is a force protection system developed initially by DMDC at the request of US Forces Korea. In brief, it uses cards, photographs and fingerprints to control access to all gates to US facilities on the Korean peninsula. All personnel having access are required to go through a registration process where biometrics are captured and cards issued to those who do not already have either CACs or other DoD issued credentials. A “one-to-many” fingerprint check is made to identify anyone already in the data base. A server based data base, which is downloaded to the gates, is available throughout Korea and is designed to operate in the absence of communications if necessary. Gate guards have wireless handheld and other devices capable of scanning a card and determining whether it is genuine and valid, bring up a photograph of the person from the data base and perform a fingerprint check in a matter of seconds. Any or all of these checks can be done depending on the threat conditions. The system notifies guards that someone should be barred or even arrested.

A version of this system is currently being installed in all US facilities in the European Command (EUCOM) Area of Responsibility (AOR). In Europe, this system is known as the Installation Access Control System (IACS). DMDC worked in coordination with the Army to make the changes necessary to meet the unique requirements of the European environment.

A further expansion of BIDS is underway in Kuwait where, in addition to the biometric technologies discussed earlier, hand geometry is being incorporated. This is because there are large numbers of local national day workers who are largely laborers that require physical

access. It is difficult to obtain quality fingerprint readings due to the type of work performed and thus an additional biometric technology has been introduced.

The common characteristic of the BIDS and its related systems is that we are moving the identity management paradigm forward. It is not enough to issue a secure identification card; you must use the technology to positively identify the person at the borders of your enterprise - whether it is for physical or logical access. A guard inspecting an ID card is simply not good enough today, when fakes are easily crafted and motivation for deception is high. The new generation of access systems use the technology embedded on the card to ensure we are granting access to the right person.

I would like to conclude my statement with a few remarks about the importance of using standards-based commercial products whenever possible. The ability to write specification in terms of well-defined and accepted national and international standards, and to have laboratories which can test products and certify that these standards have been met, ultimately reduces the cost to the users and promotes interoperability between and among Federal Agencies, business partners, and other countries. There has been a concerted effort to use such standards in the development and implementation of the CAC and both the General Services Administration (GSA) and the National Institute of Standards and Technologies (NIST) have been critical key partners in this process. Consequently, it is very easy for other organizations to adopt all or part of what DoD has done with CAC, to take advantage of multiple sources of supply based on standards, and to achieve interoperability with DoD and others. DoD and DMDC have worked

and will continue to work in conjunction with other parts of the government wanting our assistance with similar programs or to provide information on valuable lessons learned.

Thank you for the opportunity to address the Subcommittee.